Mirco Ceregato
lic. iur. HSG, LL.M., Rechtsanwalt
Partner
Co-Leiter Compliance und Investigations
Co-Leiter Prozessführung und Insolvenz
Telefon +41 58 258 14 00
mirco.ceregato@bratschi.ch

Ivan Dunjic
M.A. HSG in Law
Rechtsanwalt und öffentlicher Notar
Telefon +41 58 258 14 00
ivan.dunjic@bratschi.ch

Cyberkriminalität – Was Sie als Bank und Bankkunde wissen sollten

Cyberattacken, mittels welchen sich gewiefte Hacker beispielsweise Zugang zu E-Banking-Accounts von Privatpersonen und Unternehmen verschaffen oder Bankkundenberater über deren wahre Identität täuschen, nehmen massiv zu. Gemäss Informationen des schweizerischen Bundesamtes für Polizei fedpol sind im Jahr 2016 9'037 strafrechtlich relevante Meldungen in Bezug auf Internetkriminalität eingegangen. Im Vergleich zum Jahr 2009 stellt dies einen Anstieg von über 200% dar. In unserer anwaltlichen Beratungspraxis häufen sich konkrete Fälle mit zum Teil massiven Vermögensschäden. Betroffen davon sind sowohl Banken als auch Bankkunden. Der vorliegende Beitrag soll einen kurzen Überblick über dieses Thema verschaffen sowie erläutern, wie sich Banken und Bankkunden schützen können und welche Massnahmen sie bei Eintritt eines Schadenfalls treffen sollten.

1. Überblick

Die Vielfalt möglicher Cyberattacken ist gross. Besonders betroffen sind dabei E-Banking-Accounts von Bankkunden sowie deren Kommunikation mit ihren Bankkundenberatern. Ein häufiges Vorgehen ist dabei der Versand betrügerischer E-Mails von gefälschten Absender-Adressen oder SMS-Nachrichten, mittels welchen die Empfänger aufgefordert werden, auf einen Link zu klicken, um Ihre Login-Daten zu ändern, welche vermeintlich nicht mehr sicher seien – sog. «Phishing». Beispielsweise erhält ein Adressat eine E-Mail von einem Absender, der sich als seine Bank ausgibt. Solche Nachrichten sehen erstaunlich authentisch aus. Mit dem Klick auf den Link öffnet sich eine Internetseite, die der offiziellen Seite der Bank zum Verwechseln ähnlich sieht. Dann wird die Eingabe der E-Banking-Zugangsdaten verlangt. Werden die Zugangsdaten tatsächlich eingegeben, erhält der E-Mail-Absender die E-Banking-Zugangsdaten des Adressaten und kann so Zahlungen auslösen. Das Geld wird dabei regelmässig in Länder mit unzureichenden Geldwäschereibestimmungen verschickt, wo es anschliessend am Bankschalter in bar abgehoben oder an unzählige weitere Konten weitergeleitet werden kann.

Oft anzutreffen sind auch sog. «Man-in-the-Middle»- bzw. «Snarfing»-Angriffe, mit welchen beispielsweise Daten von Personen, die sich mit einem öffentlichen WLAN verbinden, ausspioniert werden. Illustrativ dazu folgendes Beispiel: Person X verbindet sich mit ihrem Smartphone mit einem öffentlichen WLAN-Netzwerk und loggt sich dann in ihren E-Mail-Account ein. Der Hacker

kann die E-Mail-Zugangsdaten «aufsaugen» und dann E-Mails vom tatsächlichen E-Mail-Account der Person X versenden, u.a. auch Zahlungsaufträge an die Bank der Person X.

2. Wie können sich Bankkunden schützen?

Um ihr Risiko, aufgrund von cyberkriminellen Machenschaften einen Vermögensschaden zu erleiden, minimieren zu können, können Bankkunden verschiedene Sicherheitsvorkehrungen und Vorsichtsmassnahmen treffen. Zu merken ist, dass Banken Zugangsdaten nie via E-Mail, SMS-Nachrichten oder telefonisch verlangen. Das Anklicken von Links, das Öffnen von angehängten Dateien und die Eingabe oder telefonische Mitteilung von Zugangsdaten zum eigenen E-Banking-Account sind unter allen Umständen zu unterlassen. Solche E-Mails und SMS-Nachrichten sind sofort zu löschen. Hilfreich könnte es auch sein, auf dem Computer eine Anti-Phishing-Software zu installieren. Schliesslich sind Verbindungen mit öffentlichen WLAN-Netzwerken möglichst zu vermeiden. Sind sie unvermeidbar, dann sollten während dieser Verbindung keine vertraulichen Informationen – wie zum Beispiel die Eingabe der E-Banking-Zugangsdaten – verwendet werden.

3. Welche Sorgfaltspflichten hat die Bank?

Es reicht nicht aus, dass die Bank das Risiko der Zahlung an einen Unberechtigten in ihren Allgemeinen Geschäftsbedingungen (AGB) auf ihre Kunden abwälzt. Die herrschende Rechtsprechung hält – trotz solcher Klauseln und der Wegbedingung einer Haftung – die Bank für den entstandenen Schaden des Kunden für haftbar, wenn sie die «geschäftsübliche Sorgfalt» nicht beachtet. Diesbezüglich sind die sogenannten Routinegeschäfte von den aussergewöhnlichen Bankgeschäften zu unterscheiden. Bei Zahlungsanweisungen im bisher für den Kunden üblichen Rahmen für den Bedarf von Privatpersonen oder bei Transaktionen im für die Branche üblichen Rahmen bei Geschäftskunden gelten keine erhöhten Sorgfaltspflichten seitens der Bank. Diese dürfen ohne vorherige Kontaktnahme beim Kunden ausgeführt werden, falls nicht besondere Umstände ein berechtigtes Misstrauen hervorrufen (z.B. die Zahlungsanweisung per E-Mail beinhaltet viele, für den Kunden ungewöhnliche sprachliche Fehler). Bei für den konkreten Kunden aussergewöhnlichen Bankgeschäften (z.B. Zahlungsanweisungen in hohen Beträgen, ungewöhnliche Zahlungsempfänger, Überweisung in ein „exotisches“ Land, risikoreiche Investitionen, Kredite etc.) empfehlen wir der Bank jedoch, auch ohne Vorliegen von Verdachtsgründen das Geschäft beim Kunden in geeigneter Weise zu verifizieren. Nicht adäquat ist die Verifizierung mittels dem gleichen Kanal. Wird beispielsweise eine Zahlungsanweisung vom E-Mail-Account des Kunden angewiesen, so ist die entsprechende Anweisung nicht durch eine Rückfrage per E-Mail an dieselbe oder eine andere, dem Kunden gehörende E-Mail-Adresse zu verifizieren. In diesem Fall sollte die Bank den Kunden telefonisch kontaktieren und prüfen, ob die Zahlungsanweisung auch tatsächlich von ihm stammt.

4. Was ist im Schadensfall zu tun?

Leider gelingt Cyberkriminellen der gesetzeswidrige Zugriff auf Bankkonten von Privatpersonen und Unternehmen trotz aller Sicherheitsvorkehrungen und Vorsichtsmassnahmen viel zu häufig. Wenn Bankkunden Verdacht schöpfen, dass ihre Zugangsdaten an unbefugte Dritte gelangt sein

könnten, müssen sie die Bank sofort kontaktieren und das E-Banking-Konto sperren lassen. Zusätzlich ist sofort bei der Polizei oder der Staatsanwaltschaft Anzeige zu erstatten, das elektronische Meldeformular auf der Homepage des fedpol auszufüllen sowie sämtliche Passwörter (z.B. des E-Mail-Accounts) zu ändern. Aus Sicht der Bank ist der Kunde lieber einmal mehr als weniger (vor allem telefonisch, nicht nur per E-Mail) zu kontaktieren, sofern mutmasslich dubiose Zahlungen im Raum stehen. So hält die Bank ihre Sorgfaltspflichten ein und muss nicht befürchten, bei einem allfälligen Schaden vom Kunden zivil- und/oder strafrechtlich belangt zu werden.

Da die betrügerisch überwiesenen Gelder – wie bereits erwähnt – häufig in Länder mit ungenügenden Geldwäschereibestimmungen transferiert werden, besteht die Gefahr, dass die Cyberkriminellen das Geld sehr schnell entweder in bar abheben oder aber auf diverse weitere Konten verstreuen können, so dass das betrügerisch erlangte Geld häufig nicht mehr lokalisiert werden kann. Es ist somit von essentieller Bedeutung, dass bei Verdacht auf eine Cyberattacke unverzüglich gehandelt wird. Weil in Fällen von Internetkriminalität häufig internationale Sachverhalte vorliegen und der entsprechende Rechtshilfeweg über die Polizei oder Staatsanwaltschaft in der Regel lange dauert, sollte zusätzlich umgehend ein Anwalt engagiert werden. Im Gegensatz zum behördlichen Rechtshilfeweg kann ein Anwalt in Zusammenarbeit mit Korrespondenzanwälten im Destinationsland der Zahlung eine Kontosperre in der Regel viel schneller in die Wege leiten. Zeit spielt in solchen Fällen nämlich eine entscheidende Rolle – je schneller reagiert wird, desto grösser sind die Chancen, dass das Geld wieder zurückgeholt werden kann.

Basel
Lange Gasse 15
Postfach
CH-4052 Basel
Telefon +41 58 258 19 00
Fax +41 58 258 19 99
basel@bratschi.ch

Bern
Bollwerk 15
Postfach
CH-3001 Bern
Telefon +41 58 258 16 00
Fax +41 58 258 16 99
bern@bratschi.ch

Lausanne
Avenue Mon-Repos 14
Postfach 5507
CH-1002 Lausanne
Téléfone +41 58 258 17 00
Téléfax +41 58 258 17 99
lausanne@bratschi.ch

St. Gallen
Vadianstrasse 44
Postfach 262
CH-9001 St. Gallen
Telefon +41 58 258 14 00
Fax +41 58 258 14 99
stgallen@bratschi.ch

Zug
Industriestrasse 24
CH-6300 Zug
Telefon +41 58 258 18 00
Fax +41 58 258 18 99
zug@bratschi.ch

Zürich
Bahnhofstrasse 70
Postfach
CH-8021 Zürich
Telefon +41 58 258 10 00
Fax +41 58 258 10 99
zuerich@bratschi.ch